***Kochani nauczyciele oraz rodzice ze względu na panującą epidemię, a co za tym idzie konieczność zdalnego nauczania chciałabym abyście zapoznali się z przydatnymi informacjami dotyczącymi zabezpieczania waszych danych osobowych w sieci...***

**DANE OSOBOWE BEZPIECZNE**

**PODCZAS ZDALNEGO NAUCZANIA**

**W związku z pandemią koronawirusa poczta elektroniczna i inne elementy pracy grupowej, takie jak narzędzia konferencyjne lub komunikatory internetowe stały się wsparciem dla wielu uczniów i nauczycieli, wykorzystujących zdalne metody nauczania. Korzystając z nich, warto pamiętać o bezpiecznym przetwarzaniu danych.**

**JEŚLI JESTEŚ NAUCZYCIELEM...**

─ Nauczyciel może przetwarzać dane osobowe uczniów

i ich rodziców tylko w celach związanych z wykonywaniem

swoich obowiązków służbowych.

─ Nauczyciel musi pamiętać o bezpiecznym korzystaniu

z komputerów i innych urządzeń zarówno wtedy,

gdy zapewnił mu je pracodawca, jak i wtedy, gdy korzysta

z własnych.

─ RODO nie zabrania wykorzystywania przez nauczyciela

prywatnego komputera, tabletu, czy telefonu do przetwarzania

danych osobowych w związku ze zdalnym

prowadzeniem zajęć. Urządzenia te muszą być jednak

odpowiednio zabezpieczone, a nauczyciel powinien postępować

zgodnie z polityką lub inną procedurą wprowadzoną

w tym zakresie w szkole.

─ Jeżeli nauczyciel używa własnego urządzenia, powinien

samodzielnie spełnić podstawowe wymogi bezpieczeństwa.

Przede wszystkim należy sprawdzić, czy wykorzystywane

urządzenie ma aktualny system operacyjny,

czy używane są na nim programy, w szczególności programy

antywirusowe, czy dokonane są niezbędne aktualizacje.

Na bieżąco aktualizowane powinny być także zainstalowane

programy antymalware i antyspyware. Należy rozważnie

instalować na swoich urządzeniach oprogramowanie

i pobierać je tylko z wiarygodnych źródeł (ze stron

producentów).

─ Przechowując dane na sprzęcie, do którego mogą

mieć dostęp inne osoby, należy używać mocnych haseł

dostępowych, a przed odejściem od stanowiska pracy

urządzenie powinno zostać zablokowane. Zalecane

jest także skonfigurowanie automatycznego blokowania

komputera po pewnym czasie bezczynności,

oraz założenie odrębnych kont użytkowników w przypadku

korzystania z komputera przez wiele osób.

─ Podczas korzystania z programów lub aplikacji mobilnych

należy korzystać z możliwych do zastosowania

w nich mechanizmów ochrony prywatności użytkowników.

Jeśli użycie jakiegoś programu wymaga logowania, warto

zadbać o silne hasło dostępu, a dodatkowo chronić

je przed utratą czy dostępem osób nieuprawnionych.

─ Gdy dane są przechowywane na urządzeniach przenośnych

(np. pamięć USB), muszą być bezwzględnie szyfrowane

i chronione hasłem, by zapewnić odpowiednie

bezpieczeństwo danych osobowych, w tym ochronę

przed niedozwolonym lub niezgodnym z prawem przetwarzaniem

oraz przypadkową utratą, zniszczeniem

lub uszkodzeniem.

─ W podstawowym zakresie komunikację z uczniami

i rodzicami prowadzi się poprzez wdrożone w szkole rozwiązania

teleinformatyczne, np. dzienniki elektroniczne.

W takiej sytuacji nauczyciel musi nadal zachowywać

podstawowe zasady bezpieczeństwa przy zdalnym

łączeniu się z dziennikiem elektronicznym ze swojego

urządzenia w domu.

─ Prowadzenie zajęć zdalnych może wymagać korzystania

prz ez naucz yciela z poczty ele ktronicznej

do kontaktu z uczniami lub rodzicami. Nauczyciel

powinien prowadzić taką korespondencję ze służbowej

skrzynki pocztowej, którą powinna zapewnić mu szkoła.

Jeżeli szkoła nie zapewniła nauczycielom służbowych

skrzynek poczty elektronicznej, to jeżeli wykorzystują

oni do celów służbowych prywatną skrzynkę pocztową

muszą pamiętać, aby korzystać z niej w sposób rozważny

i bezpieczny.

─ Szczególną uwagę nauczyciel musi zwrócić na zabezpieczenie

danych osobowych udostępnianych w przesyłanych

wiadomościach. Zawsze przed wysłaniem

wiadomości, należy upe wnić się , czy niezbędne

jest wysłanie danych osobowych, oraz że zamierza

wysyłać ją do właściwego adresata. Ponadto trzeba

sprawdzić, czy w nazwie adresu e-mail adresata

nie ma np. przestawionych lub pominiętych znaków

tak, aby nie wysłać takiej wiadomości do osób nieupoważnionych.

-Podczas wysyłania korespondencji

zbiorczej powinno się korzystać z opcji „UDW”,

dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie

swoich adresów e-mail.

─ Na ogólnie dostępnych portalach lub stronach internetowych

nauczyciel może jedynie publikować materiały

edukacyjne, natomiast nie może przetwarzać danych

osobowych uczniów lub rodziców.

**JEŚLI JESTEŚ RODZICEM…**

Szkoła może wymagać od ucznia jedynie danych niezbędnych

do założenia przez niego konta w odpowiednim

systemie zdalnego nauczania oraz w celu realizacji

obowiązku nauki w formie zdalnej (na podstawie

art. 35 ustawy – Prawa oświatowego w związku

z art. 6 ust. 1 lit e RODO).

─ Rodzic (opiekun prawny) ma prawo wiedzieć, jak

 administrator będzie przetwarzał dane osobowe jego

dziecka w trakcie nauki zdalnej oraz jakie w związku

z tym przysługują mu prawa.

─ Jeżeli platformy wykorzystywane do zdalnego nauczania

są odrębnymi od szkoły administratorami przetwarzanych

przez siebie danych, to rodzice i dzieci powinni

od nich otrzymać klauzulę informacyjną o podstawowych

zasadach i zakresie zbierania danych oraz administratorze,

np. podczas zakładania konta.

**Uwaga!**

**Podstawę prawną realizacji zajęć szkolnych w formie**

**pracy zdalnej określa rozporządzenie Ministra Edukacji**

**Narodowej z 20 marca 2020 r. w sprawie szczególnych**

**rozwiązań w okresie czasowego ograniczenia funkcjonowania**

**jednostek systemu oświaty w związku**

**z zapobieganiem, przeciwdziałaniem i zwalczaniem**

**COVID-19 (Dz.U. poz. 493).**

Warto przeczytać:

• ochrona danych osobowych podczas pracy zdalnej

<https://uodo.gov.pl/pl/138/1459>

• dane dzieci bezpieczne w sieci

<https://uodo.gov.pl/pl/138/1363>

• ochrona danych osobowych w szkole

<https://uodo.gov.pl/pl/383/479>

• tworzenie haseł dostępowych

<https://uodo.gov.pl/pl/138/1285>